AFCRL 716

STEP-BY-STEP DECODING IN GROUPS WITH A WEIGHT FUNCTION (PART I)

EUGENE PRANGE

PROJECT 5632
TASK 56323

AUGUST 1961

COMMUNICATION SCIENCES LABORATORY
ELECTRONICS RESEARCH DIRECTORATE
AIR FORCE CAMBRIDGE RESEARCH LABORATORIES
OFFICE OF AEROSPACE RESEARCH
UNITED STATES AIR FORCE
BEDFORD MASSACHUSETTS

ABSTRACT

Let G be a group with a weight (norm) w, and thus a distance. Let H be a normal subgroup of G. A basic lemma connects w-decomposition in G with that in the factor group G/H. One application is the justification of a general, operationally useful, concept of step-by-step decoding of G into H. A second application is to the study of a question of Slepian's: When can a set of unique coset representatives, one element of minimal weight from each H-coset, be chosen so that this set of representatives is closed under descendance? A sufficient condition, independent of H, is proved. In particular, the answer is positive for groups G with Hamming or Lee weight functions.

STEP-BY-STEP DECODING IN GROUPS WITH A WEIGHT FUNCTION (PART I)

0. INTRODUCTION

The considerations of this paper grow out of work in the theory of error-correcting code groups, but are placed in a more general context than is usual there. We consider groups with a weight function (norm) w in terms of which a distance can be defined. We are particularly interested in the theory of those cases where the triangle inequality $w(f) + w(g) \geq w(fg)$ becomes equality. A very elementary knowledge of some concepts in group theory and in the theory of order relations is assumed.

Section 1 reviews some standard properties of weight and distance on a group G, not necessarily finite or commutative. Section 2 uses the triangle equality for weight to define such concepts as w-decomposition in G and a partial ordering of G called descendance. The useful lemma (2.3) relates w-decomposition in a group G to w-decomposition in a factor group G/H. Section 3 defines and justifies step-by-step decoding, a refinement of Slepian decoding. The problem is: given some element in an H-coset, to find an element of minimal weight in that coset. Section 4 gives some results on a question of Slepian's: Given a group G with a weight function w, and a normal subgroup H of G. When is it possible to choose a set S of unique representatives for H-cosets, one element of minimal weight from each coset, such that every descendant of an element of S is also in S?

1. WEIGHT AND DISTANCE FUNCTIONS ON A GROUP

Let G be a group written multiplicatively, and with identity element e. Let w and d be mappings into the real numbers of G and of $G \times G$ respectively.

Released for publication June 22, 1961.

Given w or d, we define $\bar{d}$ or $\bar{w}$ respectively by

(1.1.1) $\bar{d}(f, g) = w(f^{-1}g)$,

(1.1.2) $\bar{w}(g) = d(e, g)$,

for all elements f, g in G.

Given such a mapping w or d, we list some properties that may or may not hold for all f, g, h in G:

(1.2.1)	$w(e)$	$= 0$;	(1.3.1)	$d(g, g)$	$=0$;
(1.2.2)	$w(g)$	> 0 if $g \neq e$;	(1.3.2)	$d(f, g)$	> 0 if $f \neq g$;
(1.2.3)	$w(g)$	$= w(g^{-1})$;	(1.3.3)	$d(f, g)$	$= d(g, f)$;
(1.2.4)	$w(f) + w(g)$	$\geq w(fg)$;	(1.3.4)	$d(f, g) + d(g, h)$	$\geq d(f, h)$;
(1.2.5)	$w(f^{-1}gf)$	$= w(g)$;	(1.3.5)	$d(fh, gh)$	$= d(f, g)$;
			(1.3.6)	$d(hf, hg)$	$= d(f, g)$.

We then have the following proposition:

(1.4) Let w be a mapping of G into the reals. Then the construction $w \xrightarrow{(1.1.1)} \bar{d} \xrightarrow{(1.1.2)} \bar{\bar{w}}$ is such that $w = \bar{\bar{w}}$ and (1.3.6) holds for $\bar{d}$. If any of the properties (1.2.1) through (1.2.5) holds for w, the corresponding property (1.3.1) through (1.3.5) holds for $\bar{d}$.

Let d be a mapping of $G \times G$ into the reals such that (1.3.6) holds. Then the construction $d \xrightarrow{(1.1.2)} \bar{w} \xrightarrow{(1.1.1)} \bar{\bar{d}}$ is such that $d = \bar{\bar{d}}$. Moreover, if any of the properties (1.3.1) through (1.3.5) holds for d, then the corresponding property (1.2.1) through (1.2.5) holds for $\bar{w}$.

We give a sample of the straightforward verifications. Suppose that (1.3.6) holds for d, to show that $d = \bar{\bar{d}}$. We have $\bar{\bar{d}}(f, g) = \bar{w}(f^{-1}g) = d(e, f^{-1}g) = d(f, g)$.

Suppose that both (1.3.6) and (1.3.4) hold for d. To show that (1.2.4) holds for $\bar{w}$, that is $\bar{w}(f) + \bar{w}(g) \geq \bar{w}(fg)$; that is, $d(e, f) + d(e, g) \geq d(e, fg)$ by the definition (1.1.2); that is, $d(f^{-1}, e) + d(e, g) \geq d(f^{-1}, g)$ using (1.3.6); but

this holds by (1.3.4).

In what follows, a mapping w with properties (1.2.1) through (1.2.5) is called a weight function on G. The corresponding mapping $\bar{d}$ of (1.1.1) is called a distance function, and will be represented by d. If the range of w is a well-ordered subset of the reals (≥ 0) in the natural ordering, we say that w is RWO. In this case, every subset S of G must have an element of least weight. In particular, if w is RWO, there is a least non-zero weight on G.

The following construction yields an interesting class of weight functions on G:

(1.5) Let A be a set of generators of a group G. Let the set A be closed under inversion and under conjugation by elements of G, that is, if a is in A and f is in G, then a^{-1} and $f^{-1}af$ are in A. Define a function w on G by: $w(e) = 0$; if $g \neq e$, $w(g)$ is the minimum length t of expressions $g = a_1 \ldots a_t$ for g as a product of elements in the generating set A. Then w is an RWO weight function.

Suppose that we are given a set of groups G_i with identity elements e_i for i in the index set I. We consider the direct product group $G = \prod_I G_i$ whose elements are the sets $g = (g_i)$, where each component g_i of g is in G_i, and where the relation $g_i = e_i$ holds for all except a finite number of components. Multiplication is defined by $fg = h$, where $h_i = f_i g_i$. We then have

(1.6) Let $G = \prod G_i$ be a direct product of groups G_i with weight functions w_i. Then

(1.6.1) $$w(g) = \sum_i w_i(g_i)$$

defines a weight function w on G.

We mention some special classes of weight functions as examples. They can be defined either through (1.5) or (1.6).

(1.7.1) If we take A = G in (1.5), the group is said to have the coarse weight function. All elements other than the identity then have weight 1.

(1.7.2) Let G be a direct product group. Take A in (1.5) as the set of all elements g such that $g_i = e_i$ for every component except one. The group G is then said to have a Hamming weight function. Equivalently, give the groups G_i coarse weight functions w_i, and define the weight function on G by (1.6).

(1.7.3) Let G be a direct product of cyclic groups G_i, each with a fixed generating element b_i. Take A as the set of all elements g such that $g_i = e_i$ for every component except one, this component g_j being either b_j or b_j^{-1}. The group G is then said to have a Lee weight function.

The following properties deal with a subgroup of a group with weight function.

(1.8) Let the group G have an RWO weight function w, and let H be a normal subgroup of G. Then an RWO weight function on the factor group G/H is defined by w(Z) = min w(z) for z in Z, where Z is any H-coset.

If we do not require w on G to be RWO, and define w(Z) = inf w(z) for z in Z, then the function w on G/H does not necessarily satisfy (1.2.2).

(1.9) Let G be a group with a weight function w and the corresponding distance function d. Let H be any subgroup of G, and g be any element of G. Then d(h, g) is minimal for h in H if and only if $h = gf^{-1}$, where f is some element of minimal weight in the coset Hg.

By definition, $d(h, g) = w(h^{-1}g)$. Then $f = h^{-1}g$ runs through the coset Hg as h runs through the group H.

Remarks. Slepian (1956) has made property (1.9) the basis of a decoding procedure for error-correcting group codes. See also Hamming (1950) and Lee (1958).

2. w-DECOMPOSITION

Let G be a group with a weight function w. We say that a relation $[g; g_1, \ldots, g_t]$ holds in G and defines a w-decomposition of g if

$$(2.1) \qquad \begin{cases} g = g_1 \cdots g_t, \\ w(g) = w(g_1) + \ldots + w(g_t), \end{cases}$$

for g, g_i in G. The relations $[g; g_1, \ldots, g_t]$ and $[g_i; h_1, \ldots, h_s]$ imply $[g; g_1, \ldots, g_{i-1}, h_1, \ldots, h_s, g_{i+1}, \ldots, g_t]$.

A w-decomposition of g is called trivial if one of the factors g_j of (2.1) is equal to g, the other factors then necessarily being equal to the identity element e of G. We call $g \neq e$ in G an atom if all w-decompositions of g are trivial. We call a w-decomposition of g atomic if all the factors g_i of the decomposition are atoms. An atomic w-decomposition of an element g in G necessarily exists if w is RWO. An example at the end of this section shows that the set of atoms occurring in an atomic w-decomposition of g need not be uniquely determined by g.

Any factor g_i occurring in any w-decomposition of g is called a descendant of g, the factors g_1 and g_t of (2.1) being called left and right descendants respectively. An element f is a right descendant of g if and only if $w(g) = w(gf^{-1}) + w(f)$.

We write $f \leq g$ if f is a descendant of g. The relation of descendance gives a partial ordering of g (as do the relations of left or right descendance), that is,

$$(2.2) \qquad \begin{cases} f \leq g \text{ and } g \leq f \text{ if and only if } f = g, \\ f \leq g \text{ and } g \leq h \text{ imply } f \leq h. \end{cases}$$

An atom of G can be described as an element $g \neq e$ whose only descendants are g and e. The atoms in the construction (1.5) are the elements unequal to e in the generating set A.

The following useful lemma relates w-decomposition in a group G to that in a factor group G/H:

(2.3) Given a normal subgroup H of a group G with an RWO weight function w, let the factor group G/H have the induced weight function w of (1.8).
(2.3.1) If z is an element of minimal weight in the coset $Z = Hz$ and if the relation $[z; z_1, \ldots, z_t]$ holds in G, then each z_i, $1 \leq i \leq t$, is an element of minimal weight in the coset $Z_i = Hz_i$, and the relation $[Z; Z_1, \ldots, Z_t]$ holds in G/H.
(2.3.2) Conversely, if the relation $[Z; Z_1, \ldots, Z_t]$ holds in G/H and if z_i is an element of minimal weight in Z_i, $1 \leq i \leq t$, then $z = z_1 \ldots z_t$ is an element of minimal weight in Z, and the relation $[z; z_1, \ldots, z_t]$ holds in G.

To prove (2.3.1), it follows from the definition (1.8) of the induced weight function on G/H that $w(Z_i) \leq w(z_i)$, $1 \leq i \leq t$. Thus

$$\begin{aligned} w(Z_1) + \ldots + w(Z_t) &\leq w(z_1) + \ldots + w(z_t) \text{ by (1.8)}, \\ &= w(z) = w(Z) \quad \text{by hypothesis}, \\ &\leq w(Z_1) + \ldots + w(Z_t) \quad \text{by the triangle inequality (1.2.4) on G/H.} \end{aligned}$$

Since the extreme terms are identical, there must be equality throughout. The first equality implies the set of equalities $w(Z_i) = w(z_i)$.

To prove (2.3.2), we have

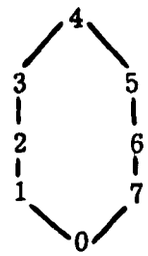
$$\begin{aligned} w(z) &\leq w(z_1) + \ldots + w(z_t) && \text{by (1.2.4) on G}, \\ &= w(Z_1) + \ldots + w(Z_t) = w(Z) && \text{by hypothesis}, \\ &\leq w(z) && \text{by (1.8)}. \end{aligned}$$

Since the extreme terms are identical, there is equality throughout, and the converse holds.

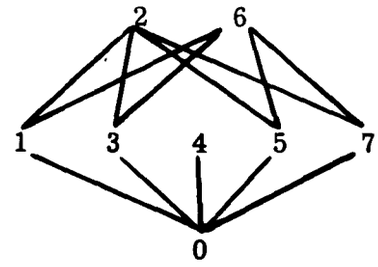
We give some concrete illustrations of weight functions. Let G be the cyclic group of order 8 written as the group of integers with addition modulo 8. We give two weight functions w and $\tilde{w}$ on G in the following table.

g	0	1	2	3	4	5	6	7
w(g)	0	1	2	3	4	3	2	1
$\tilde{w}$(g)	0	1	2	1	1	1	2	1

Both weight functions are examples of construction (1.5) with the generating set A as the set of elements of weight 1 in the table. The weight function w is a Lee weight function (1.7.3). The atomic $\tilde{w}$-decompositions of the elements 2 and 6 in $(G, \tilde{w})$ are $2 = 1+1 = 5+5 = 3+7$, $6 = 3+3 = 7+7 = 1+5$. The partial ordering of descendance in the two cases is represented in the following diagrams.



(G, w)



$(G, \tilde{w})$

3. STEP-BY-STEP DECODING

Here G is a group with a RWO weight function w, H is a normal subgroup of G, and the factor group G/H has the induced weight function w of (1.8). We call H a code group. We call a mapping $g \to g'$ of G into H a

decoding function if $d(g, g') \leq d(g, h)$ for all h in H. A decoding function maps each g of G into a closest element g' in H.

The word classifying can replace decoding here. For each element h in the subgroup H, let $S(h)$ be the set of all elements g in G that are as close to h as to any other element of H. Then to decode an element g of G into a closest element h of H is to determine that g belongs to the class $S(h)$.

Consider a mapping of G into H,

$$g \to g' = gf^{-1}, \tag{3.1}$$

where f is some element of minimal weight in the coset Hg. Then by (1.9), the mapping (3.1) is a decoding function.

The concept of step-by-step decoding to be introduced adds nothing in theory to what has just been said. It is of interest if an operational point of view is taken. It may be thought of as justifying the piece-by-piece construction of an element f of minimal weight in the coset Hg, going from an element g of G to a closest code element g' of H in a series of steps.

Consider a mapping of G into G,

$$g \to gz^{-1}, \tag{3.2}$$

where z is a right descendant of some element of minimal weight in the coset Hg, z being the identity e of G if and only if $Hg = H$. Consider a chain formed by applications of this mapping,

$$g = g_0 \to g_1 \to g_2 \to \cdots, \tag{3.3}$$

where $g_{i+1} = g_i z_i^{-1}$ as in (3.2). We wish to prove:

(3.4) There is a first element g_j in the chain (3.3) such that g_j is in H. The mapping $g \to g_j$ is a decoding function for G over the code group H.

Proof. Let $Y_i = Hg_i$, and $Z_i = Hz_i$. Since by definition z_i is a right descendant of an element of minimal weight in Y_i, it follows from (2.3.1)

that z_i is an element of minimal weight in the coset Z_i, and that the relation $[Y_i; Y_{i+1}, Z_i]$ holds in G/H. Thus for all i, the relation $[Y_0; Y_{i+1}, Z_i, Z_{i-1}, \ldots, Z_0]$ holds, and each z_i is an element of minimal weight in Z_i. Since the weight function is RWO, there must exist some index j such that $Y_j = H$. Let $f = z_{j-1} z_{j-2} \cdots z_0$. Then the relation $[Y_0; Z_{j-1}, \ldots, Z_0]$ holds, and by (2.3.2) the relation $[f; z_{j-1}, \ldots, z_0]$ holds in G, and f is an element of minimal weight in $Y_0 = Hg$. Thus, $g_j = gf^{-1}$ is an element of H at minimal distance from g, completing the proof of (3.4).

Note that the elements $z \neq e$ of (3.2) can be restricted to be atoms of G. Note also that in (3.1) or (3.2) the element f or z can be required to be the same for every g in an H-coset.

Remark. The concept of step-by-step decoding is regarded here as a refinement of the decoding principle introduced in Slepian (1956). A planned second part to the present paper will consider concrete applications. Some concrete examples can be found in Prange (1958, 1959). See also Wells (1960) and Peterson (1961).

4. SUBSETS CLOSED UNDER DESCENDANCE

We say that a subset S of a group G with weight function w is closed under descendance if for every element g of S, all descendants of g are in S. For example, if H is a normal subgroup of G and if S is the set of all elements of G that are of minimal weight in their H-coset, then the first half of (2.3) guarantees that S is closed under descendance.

Given (g, w) and a normal subgroup H of G, is it possible to choose a set S of coset representatives, exactly one element of minimal weight from each H-coset, such that the set S is closed under descendance? This cannot always be done, as the following counterexample shows. Let $(G, \tilde{w})$ be the group of

integers under addition modulo 8 with the weight function $\tilde{w}$ of Sec. 2. Let H be the subgroup $\{0, 4\}$. Since one of the elements 2 or 6 must be chosen as a representative of the coset $H + 2 = \{2, 6\}$, a set of representatives for H-cosets must contain at least the six descendants of this element if the set is closed under descendance. But there are only four H-cosets.

The results to be proved are as follows. We prove (4.1) a sufficient condition (independent of H) that the answer to the above question be positive. We show (4.2) that this sufficient condition holds in a finite or countable direct product of groups each of which satisfies the condition. Finally we show (4.3) that the condition holds in the basic groups used in defining direct product groups with Lee or Hamming weight.

(4.1) Let (G, w) have a well-ordering $<<$ such that

(4.1.1) $w(x) < w(y)$ implies that $x << y$; and

(4.1.2) if the relations $[z; w, x, y]$ and $[\bar{z}; w, \bar{x}, y]$ hold in G, then $\bar{x} << x$ implies $\bar{z} << z$.

If C is any subset of G, let C* be the least element of C under the well-ordering $<<$. Then for every normal subgroup H of G, the set S(H) of all representatives Z* for cosets Z in the factor group G/H is a set of unique coset representatives of minimal weight that is closed under descendance.

Proof. The relations $[z; w, x, y]$ and $[\bar{z}; w, \bar{x}, y]$ imply that $w(z) - w(\bar{z}) = w(x) - w(\bar{x})$. Thus if an ordering satisfies (4.1.1), it automatically satisfies (4.1.2) in all cases where $w(x) \neq w(\bar{x})$. Note also that any well-ordering of G that satisfies (4.1.1) is an extension of the partial ordering of descendance. The existence of a well-ordering satisfying (4.1.1) implies that w is RWO.

We must show that, given the normal subgroup H, the set S(H) is closed under descendance. Let Z be an H-coset, $Z^* = z$, and let x be a descendant of z. Then for some elements w and y, the relation $[z; w, x, y]$ holds in G.

Let $Hw = W$, $Hx = X$ and $Hy = Y$. By (2.3.1), the relation $[Z; W, X, Y]$ holds in G/H, and w, x, and y are elements of minimal weight in W, X, and Y respectively. Suppose that x is not in S(H), that is, $X^* = \overline{x} << x$. Let $\overline{z} = w\ \overline{x}\ y$. By (2.3.2), $\overline{z}$ is an element (of minimal weight) in Z, and the relation $[\overline{z}; w, \overline{x}, y]$ holds in G. By hypothesis (4.1.2), $\overline{z} << z$ since $\overline{x} << x$, a contradiction. Thus $X^* = x$, and the set S(H) is closed under descendance.

(4.2) Let $G = \prod_I G_i$ be the direct product of a finite or countable number of groups (G_i, w_i) for each of which the hypothesis of (4.1) holds. Let the weight function w on G defined by (1.6) be RWO. Then the hypothesis of (4.1) holds for (G, w).

Proof. We may assume that the index set I is either the set of positive integers, or a finite initial segment 1, 2, ... , n of this set. By hypothesis, each group (G_i, w_i) has a well-ordering << that satisfies (4.1.1) and (4.1.2). We define an ordering on (G, w) as follows: $x << \overline{x}$ if (4.2.1) $w(x) < w(\overline{x})$, or if (4.2.2) $w(x) = w(\overline{x})$, $x_i = \overline{x}_i$ for $i > j$, and $x_j << \overline{x}_j$. Recall that for any element $x = (x_i)$ of G, $x_i = e_i$ for all except a finite number of components. Thus, for any two elements $x \neq \overline{x}$ of G, there must exist a greatest integer j such that $x_j \neq \overline{x}_j$. The ordering << on G is at least a simple ordering, any two elements of G are comparable.

We must show that the ordering << on G is a well-ordering, that is, every nonempty subset C of G has a least element C*. The following construction of nested subsets of C clearly leads to a least element. Choose first the elements c of minimal weight in C. These exist, since the weight function on G is RWO by hypothesis. Of these, choose those elements c for which the integer j such that $c_i = e_i$ for all $i > j$ is minimal. Of these choose the elements c such that, successively, $c_j, c_{j-1}, \ldots, c_1$ are least

in the given orderings of $G_j, \ldots, G_1$.

Our definition guarantees that (4.1.1) holds for the ordering << on G. We proved that if $w(x) \neq w(\bar{x})$, then (4.1.1) implies (4.1.2). In the case $w(x) = w(\bar{x})$, suppose that the relations $[z; w, x, y]$ and $[z; w, \bar{x}, y]$ hold on G. Then the highest integer j for which x_j and $\bar{x}_j$ disagree is the same as the highest integer j for which z_j and $\bar{z}_j$ disagree. In this case, the definition (4.2.2) reduces the verification of (4.1.2) on G to its verification on G_j, where it holds by hypothesis. This completes the proof of (4.2).

(4.3) The hypothesis of (4.1) can be satisfied for groups (G, w) of the following types: (4.3.1) any group with coarse weight function for which some well-ordering exists; (4.3.2) any cyclic group with weight function defined by (1.5) for a set $A = \{b, b^{-1}\}$ of generators. Indeed, in these cases, any well-ordering that satisfies (4.1.1) automatically satisfies (4.1.2).

Proof. It is clear that in either of these cases, a well-ordering satisfying (4.1.1) exists. We wish to show that such an ordering also satisfies (4.1.2). We need only consider the case $z \neq \bar{z}$, $w(z) = w(\bar{z})$. Suppose we have verified in this case that the only common descendant of z and $\bar{z}$ is the identity element e of G. Then in the hypothesis of (4.1.2), we must have $w = y = e$, whence $x = z$ and $\bar{x} = \bar{z}$, and (4.1.2) holds. If the group has coarse weight function, all elements other than the identity are atoms, and two distinct atoms have only e as a common descendant. If the group is a cyclic group with the given weight function, then there are at most two elements b^t and $(b^{-1})^t$ of weight t. If these elements are distinct, then the set of descendants of the first element contains exactly the elements b^i for $0 \leq i \leq t$; and similarly for the second. If these sets have more than the element e in common, then the expressions b^t and $(b^{-1})^t$ cannot be minimal expressions in the generators. Thus our supposition

holds in both cases.

It now follows, working backward, that the hypothesis and conclusion of (4.1) can be satisfied for groups with Hamming or Lee weight, provided that direct products of an at most countable number of basic groups are allowed, and that each of the basic groups in the Hamming weight case can be well-ordered.

Remark. Slepian conjectured that the answer to the question considered in this section was positive for a finite direct product of two-element groups, and this was proved by E. F. Moore (unpublished, 1957). An affirmative answer in the case of Lee weight was given by Prange (unpublished, 1959) and it is this proof that is given above in a more abstract form. The question is an interesting one, but I do not know of any application. See also Peterson (1961).

REFERENCES

HAMMING, R.W., Error detecting and error correcting codes. Bell System Tech. J. 29:147-160 (1950).

LEE, C.Y., Some properties of nonbinary error-correcting codes. IRE Trans. IT-4:77-82 (1958).

PETERSON, W.W., Error-correcting Codes. M.I.T. Press and Wiley (1961).

PRANGE, E., Some Cyclic Error-correcting Codes With Simple Decoding Algorithms. AFCRC-TN-58-156, Air Force Cambridge Research Center (1958).

PRANGE, E., The Use of Coset Equivalence in the Analysis and Decoding of Group Codes. AFCRC-TR-59-164, Air Force Cambridge Research Center (1959).

SLEPIAN, D., A class of binary signalling alphabets. Bell System Tech. J. 35:203-234 (1956).

WELLS, W.I., Decoding of Group Codes for Binary Symmetric Channels. M.I.T. Lincoln Lab. Rpt 22G-0029 (1960).

UNCLASSIFIED

AF Cambridge Research Laboratories, Bedford, Mass. Electronics Research Directorate
STEP-BY-STEP DECODING IN GROUPS WITH A WEIGHT FUNCTION (PART I), by Eugene Prange. August 1961. 13pp. AFCRL 716
Unclassified report

Let G be a group with a weight (norm) w, and thus a distance. Let H be a normal subgroup of G. A basic lemma connects w-decomposition in G with that in the factor group G/H. One application is the justification of a general, operationally useful, concept of step-by-step decoding of G into H. A second application is to the study of a question of Slepian's: When can a set of unique coset representatives, one element of minimal weight from each H-coset, be chosen so that this set of representatives is closed under descendance? A sufficient condition, independent of H, is proved. In particular, the answer is positive for groups G with Hamming or Lee weight functions.

1. Group theory—groups with weight functions
2. Coding theory—step-by-step decoding
3. Classification theory
I. Prange, E.

UNCLASSIFIED

UNCLASSIFIED

AF Cambridge Research Laboratories, Bedford, Mass. Electronics Research Directorate
STEP-BY-STEP DECODING IN GROUPS WITH A WEIGHT FUNCTION (PART I), by Eugene Prange. August 1961. 13pp. AFCRL 716
Unclassified report

Let G be a group with a weight (norm) w, and thus a distance. Let H be a normal subgroup of G. A basic lemma connects w-decomposition in G with that in the factor group G/H. One application is the justification of a general, operationally useful, concept of step-by-step decoding of G into H. A second application is to the study of a question of Slepian's: When can a set of unique coset representatives, one element of minimal weight from each H-coset, be chosen so that this set of representatives is closed under descendance? A sufficient condition, independent of H, is proved. In particular, the answer is positive for groups G with Hamming or Lee weight functions.

1. Group theory—groups with weight functions
2. Coding theory—step-by-step decoding
3. Classification theory
I. Prange, E.

UNCLASSIFIED

UNCLASSIFIED

AF Cambridge Research Laboratories, Bedford, Mass. Electronics Research Directorate
STEP-BY-STEP DECODING IN GROUPS WITH A WEIGHT FUNCTION (PART I), by Eugene Prange. August 1961. 13pp. AFCRL 716
Unclassified report

Let G be a group with a weight (norm) w, and thus a distance. Let H be a normal subgroup of G. A basic lemma connects w-decomposition in G with that in the factor group G/H. One application is the justification of a general, operationally useful, concept of step-by-step decoding of G into H. A second application is to the study of a question of Slepian's: When can a set of unique coset representatives, one element of minimal weight from each H-coset, be chosen so that this set of representatives is closed under descendance? A sufficient condition, independent of H, is proved. In particular, the answer is positive for groups G with Hamming or Lee weight functions.

1. Group theory—groups with weight functions
2. Coding theory—step-by-step decoding
3. Classification theory
I. Prange, E.

UNCLASSIFIED

UNCLASSIFIED

AF Cambridge Research Laboratories, Bedford, Mass. Electronics Research Directorate
STEP-BY-STEP DECODING IN GROUPS WITH A WEIGHT FUNCTION (PART I), by Eugene Prange. August 1961. 13pp. AFCRL 716
Unclassified report

Let G be a group with a weight (norm) w, and thus a distance. Let H be a normal subgroup of G. A basic lemma connects w-decomposition in G with that in the factor group G/H. One application is the justification of a general, operationally useful, concept of step-by-step decoding of G into H. A second application is to the study of a question of Slepian's: When can a set of unique coset representatives, one element of minimal weight from each H-coset, be chosen so that this set of representatives is closed under descendance? A sufficient condition, independent of H, is proved. In particular, the answer is positive for groups G with Hamming or Lee weight functions.

1. Group theory—groups with weight functions
2. Coding theory—step-by-step decoding
3. Classification theory
I. Prange, E.

UNCLASSIFIED

AD

UNCLASSIFIED

UNCLASSIFIED

AD

UNCLASSIFIED

UNCLASSIFIED

AD

UNCLASSIFIED

UNCLASSIFIED

AD

UNCLASSIFIED

UNCLASSIFIED